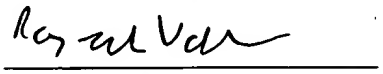
Remarks

New claims 438-585 are added and the abstract is revised. No new matter has been added.

Respectfully submitted,



Rajesh Vallabh
Reg. No. 35,761

Hale and Dorr LLP
60 State Street
Boston, MA 02109
617-526-6505

January 2, 2003

Attorney Docket No.: 112.634.120

Attachments: "Clean" versions of added claims and replacement abstract

Original abstract blacklined to show amendments

Blacklined Version of Replacement Abstract

Abstract of the Invention

[(Fig. 2)]

An Information Management System

An information management system is described including **[comprising]** one or more workstations running applications to allow a user of the workstation to connect to a network, such as the Internet. Each application operates in conjunction with **[has]** an **[analyser]** analyzer, which monitors transmission data that the application is about to transmit to the network or about to receive from the network and which determines an appropriate action to take regarding that transmission data. Such actions may be extracting data from the transmission data, such as passwords and usernames, digital certificates or eCommerce transaction details for storage in a database; ensuring that the transmission data is transmitted at an encryption strength appropriate to the contents of the transmission data; determining whether a check needs to be made as to whether a digital certificate received in transmission data is in force, and determining whether a transaction about to be made by a user of one of the workstations needs third party approval before it is made. The **[analyser]** analyzer may consult a policy data containing a policy to govern the workstations in order to make its determination.

The information management system provides many advantages in the eCommerce environment to on-line trading companies, who may benefit from improvements to record-keeping, security and control over **[by being able to regulate]** the transactions **[made by their staff according to their instructions in a policy data, automatically maintain records of passwords and business conducted on-line, avoid paying for unnecessary checks on the validity of digital certificates and ensure that transmissions of data made by their staff are always protected at an agreed strength of encryption]**.